

UNITED STATES DISTRICT COURT

for the
Western District of Oklahoma

FILED
NOV 09 2023
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.
BY KS DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE CELLULAR
DEVICE ASSIGNED CALL NUMBER (405) 679-8310 IN
THE CUSTODY OR CONTROL OF T-MOBILE

Case No. M-23- 927-AMG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the WESTERN District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section
18 U.S.C. § 2252A

Offense Description
Receive, Distribute, and Possess Child Pornography

The application is based on these facts:

See Affidavit, attached hereto

- ☒ Continued on the attached sheet.
☒ Delayed notice of 365 days (give exact ending date if more than 30 days: 11/09/2024) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Shane Robinson, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date:

11/9/2023City and state: Oklahoma City, Oklahoma


Judge's signature

AMANDA MAXFIELD GREEN, U.S. MAGISTRATE JUDGE
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA**

**IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH THE CELLULAR DEVICE
ASSIGNED CALL NUMBER (405) 679-
8310 IN THE CUSTODY OR
CONTROL OF T-MOBILE**

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, **Shane Robinson**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular device assigned with call number **(405) 679-8310** (the “**TARGET CELLPHONE**”) that is in the custody or control of **T-MOBILE**, a wireless communications service provider that accepts process at **4 SYLVAN WAY, PARSIPPANY, NEW JERSEY 07054**. As a provider of wireless communications service, **T-MOBILE** is a provider of “electronic communications service,” as defined in 18 U.S.C. § 2510(15).

2. The information to be searched is described in the following paragraphs and in **Attachment A**. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require **T-MOBILE** to disclose to the government the information further described in Section I of **Attachment B**. Upon receipt of the information described in Section I of

Attachment B, government-authorized persons will review the information to locate the items described in Section II of **Attachment B**.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definition of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act, *see* 18 U.S.C. §§ 3121–3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute, including a certification from an attorney for the government that the information likely to be obtained by the requested pen register and trap-and-trace device is relevant to an ongoing criminal investigation. *See* 18 U.S.C. § 3123(b)(1). That certification is attached as **Attachment C**.

4. In sum, this affidavit is made in support of an application for three distinct items: (1) a pen register and trap-and-trace device on the **TARGET CELLPHONE**, pursuant to 18 U.S.C. § 3121–3127; (2) a “ping” on the **TARGET CELLPHONE**, pursuant to 18 U.S.C. § 2703 and Fed. R. Crim. P. 41(c); and (3) an order for historical and prospective cell site data for the **TARGET CELLPHONE**, pursuant to 18 U.S.C. § 2703(d).

5. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since April 23,

2023. In this capacity, my responsibilities include the investigation of possible violations of federal law, including the investigation of traders/distributors of child sexual abuse material. During my career, my investigations have included the use of various surveillance techniques and the execution of various search, seizure, and arrest warrants.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 2252A, receipt, distribution and possession of child pornography, has been committed by **KRAIG VARNEY (VARNEY)**. There is probable cause to search the information described in **Attachment A** to assist and aid in the location of **VARNEY** as further described in **Attachment B**.

8. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. §§ 2711 & 3127. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. §§ 2711(3)(A)(i) & 3127(2)(A)(i).

PROBABLE CAUSE

9. Law enforcement, including the FBI, is conducting a criminal investigation into the possession and distribution of child pornography in the Western District of Oklahoma. **VARNEY** has been identified as the individual knowingly using Kik to receive, distribute, and possess child pornography.

10. This case originated on October 24, 2023, when your affiant received a lead from FBI Tampa Division, Sarasota Resident Agency. During their investigation, agents accessed a subject's cellular device. On this device were conversations from an unidentified Kik group, which appeared to focus on the trading of videos and pictures of child sexual abuse material (CSAM).

11. Kik is a social media smartphone application that can be used to exchange text, images, and videos. The app usually requires users to register a unique user screen name. The registration process for this app requires the user to provide contact information to register their screen name, such as an email address or phone number.

12. On or about April 28, 2023, the Kik username "Okcsparky" posted multiple CSAM thumbnail pictures to this Kik group. One of the unidentified users in this group commented "Anymore rough ones?", to which "Okcsparky" replied "Idk... I'm driven it's hard to look through my shit". After these comments, "Okcsparky" posted multiple CSAM thumbnail pictures to the group.

13. On August 14, 2023, FBI Tampa Division issued an administrative subpoena to Kik, to provide information pertaining to subscriber information and IP logs associated with the username "Okcsparky" from April 27, 2023, to August 14, 2023.

14. On August 16, 2023, FBI Tampa Division received Kik's response to the administrative subpoena with the following information regarding "Okcsparky": email address: kraigvarney76@gmail.com; First Name: moving; Last Name: Left. On the date of the CSAM postings described in paragraph 11, "Okcsparky" utilized the IP address 68.12.212.15 to login to Kik. This IP address resolved to Cox Communications (Cox).

15. On August 31, 2023, FBI Tampa Division issued an administrative subpoena to Cox, to provide information pertaining to subscriber information associated to the following: IP address 68.12.212.15, Port: 36078, Date: 2023-04-28 19:57:31 UTC 68.12.212.15, Port: 58504, Date: 2023-04-28 19:59:55 UTC 68.12.212.15, Port: 58808, Date: 2023-04-28 20:01:46 UTC.

16. On September 11, 2023, FBI Tampa Division received Cox's response to the administrative subpoena with the following information regarding the subscriber of the IP address 68.12.212.15, on the requested timeframe described above:

Name:	Kelly Watson
Address:	8300 NW 10th St, Apt 2, Oklahoma City, Oklahoma 73127
Phone:	(405) 627-8919 (405) 761-1802
E-Mail:	kellyin.pink@gmail.com

17. A search of Oklahoma Department of Public Safety provided current driver's license photo and residential information for Kelly Watson (Watson) who resides at 8300 Northwest 10th Street, Oklahoma City, Oklahoma 73127.

18. On November 1, 2023, your affiant conducted an open-source search and identified a Facebook account for Kelly Watson who states on her account that she resides in Oklahoma City, Oklahoma. Upon review, there were multiple photos of Watson. The Facebook photos and the driver's license photo appear to show the same person, which is Kelly Watson. Furthermore, Watson's email address kellyin.pink@gmail.com is similar to Kelly Watson's Facebook account, www.facebook.com/kellyin.pink.

19. On November 1, 2023, your affiant searched the Oklahoma Department of Corrections (DOC) database for VARNEY. According to VARNEY's criminal history, he served time in prison for drug trafficking and firearms related charges. VARNEY, born October 3, 1976, had several booking photographs in the database, including one photograph which showed the upper portion of a tattoo on VARNEY's chest. VARNEY is pictured in numerous photographs on Watson's Facebook account, including one photograph that shows his chest tattoo from the DOC database.

20. Your affiant believes Kraig VARNEY is the owner and user of the email address kraigvarney76@gmail.com and that he used this email to register his account with Kik referenced in paragraph 14.

21. On October 25, 2023, FBI Tampa Division followed FBI CSAM protocols and securely transferred CSAM which was distributed by "Okcsparky" in a Kik group text. Your affiant reviewed all of the images/videos, including CSAM, provided by FBI Tampa Division. Based on the training and experience of other law enforcement officers and my own research, it was determined that several of the files depict children under the age of eighteen years engaged in sexual acts or lascivious exhibitions of the genitals that constitute child pornography as defined by Title 18 U.S.C. § 2256. A few of the files are described below:

a. Filename: c3546efd4c246975c86b886a4ab18e8b

Description: This image depicts a nude prepubescent female lying on her back with her legs spread open and up in the air. She has what appears to be a pencil shaped object in her hand penetrating her vagina. There appears to be an adult hand penetrating her anal cavity with an index finger.

b. Filename: 61ff8a7394609d6bcf2c88644cfb06d6

Description: This image depicts a prepubescent female, wearing what appears to be a swimsuit with pinkish purple and white stripes, laying on her back being penetrated by an erect penis while the male's hand is pressing down on her stomach.

c. Filename: d26f218b696fc17a05549d9c4d6ef84

Description: This image depicts a nude prepubescent female laying next to a nude adult male, both are lying on their backs, and another nude female is on her knees hovering over the male. The nude adult male has his arm wrapped around the nude prepubescent female with his hand placed on her vagina and his other arm is wrapped around the thigh of the nude female hovering over him.

d. Filename: 383cb4fd49ef0f9fld89dec217414784

Description: This image depicts a prepubescent female with her hands grabbing her butt as she places her index finger on her anal cavity, while a toothbrush is protruding upright out of her vagina.

22. Your affiant conducted postal checks and it was confirmed that VARNEY receives mail at 12324 South Land Avenue, Oklahoma City, Oklahoma, 73170.

VARNEY does not receive mail at 8300 North West 10th Street, Oklahoma City, Oklahoma 73127. On October 30, November 3, November 8, and November 9, 2023, law enforcement did reconnaissance at the 12324 South Land Avenue property, but did not observe VARNEY, or his vehicle, believed to be a red 2016 Toyota Corolla, license plate MNR983, at the residence.

23. On November 7, 2023, your affiant interviewed M.O., VARNEY's probation officer, at Department of Corrections, 1919 Industrial Boulevard, Norman, Oklahoma 73069. M.O. provided Varney's cellular telephone number, (405) 679-8310

(**TARGET CELLPHONE**), and his employment information at Oklahoma Electrical Supply Company, located in Tulsa, Oklahoma. M.O. contacts **VARNEY** via the **TARGET CELLPHONE** to schedule Home Visits and in person visits at Department of Corrections, Norman, Oklahoma.¹

24. Through database checks, I have confirmed that **T-MOBILE** provides service for the **TARGET CELLPHONE**. In my training, and experience of other law enforcement officers, I have learned that **T-MOBILE** is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be ten (10) or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

¹ The government is requesting cell site data for forty-five days. This additional information will be useful in establishing a pattern of life, which is necessary to establish anomalous behavior. In my training, and experience of other law enforcement officers, getting the context of cell site data is necessary in order to better understand the significance of any one particular point of data.

25. Based on my training, and the experience of other law enforcement officers, I know that **T-MOBILE** can collect cell-site data about the **TARGET CELLPHONE**. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; (5) the cell tower roundtrip network measurements from tower to device and back to tower, commonly referred to as Timing Advance data; and (6) the duration of the communication. I also know that wireless providers such as **T-MOBILE** typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

26. Based on my training, and the experience of other law enforcement officers, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers—as transmitted from a cellular device to a cellular antenna or tower—can be

recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

27. Based on my training, and the experience of other law enforcement officers, I know wireless providers such as **T-MOBILE** typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as **T-MOBILE** typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training, and experience of other law enforcement officers, this information may assist in locating **VARNEY**. In my training, and experience of other law enforcement officers, this information may also constitute evidence of the crimes under investigation because the information can be used to identify the **TARGET CELLPHONE**'s user or users.

28. Based on my training, and the experience of other law enforcement officers, the combination of both historical and prospective location information is helpful in locating individuals. The historical location information from cellular phones can help establish a pattern of life, while prospective location information—including cell-site information, phone pings, and timing advance measurements/distance-to-tower measurements—can help provide more precise real-time information regarding the

location of the **TARGET CELLPHONE**'s user. To help ensure that **VARNEY** is located, I am requesting precise location information for the next forty-five (45) days for the **TARGET CELLPHONE**.

AUTHORIZATION REQUEST

29. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Fed. R. Crim. P. 41. The proposed warrant will also function as a pen register order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and/or trap and trace device to record, decode, and/or capture certain information in **Attachment A** for each communication to or from the **TARGET CELLPHONE**, without geographic limit, for a period of forty-five (45) days pursuant to 18 U.S.C. § 3123(c)(1).

30. I further request, pursuant to 18 U.S.C. § 2703(b)(1)(A), that the Court find that the government is not required to provide notice of this warrant to the subscriber, customer, or person who was monitored. I also request, pursuant to 18 U.S.C. § 3123(d), that **T-MOBILE** be ordered not to disclose to the listed customer or any other person the existence and/or use of the pen register and trap-and-trace device sought herein. Additionally, there is reasonable cause to believe that providing immediate notification of the warrant to the subscriber, customer, or person who is being monitored may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber, customer, or user of the **TARGET CELLPHONE** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and

flee from prosecution. *See* 18 U.S.C. § 2705(a)(2). Therefore, I request that the Court order **T-MOBILE** not to notify any other person of the existence of this warrant and order for a period of one year from the date the requested warrant is issued, except that the service provider may disclose this warrant and order to an attorney for the service provider for the purpose of receiving legal advice. As further specified in **Attachment B**, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

31. I further request that the Court direct **T-MOBILE** to disclose to the government any information described in Section I of **Attachment B** that is within its possession, custody, or control. Because the warrant will be served on **T-MOBILE**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed for a period of twelve months from the date the requested warrant is issued, or until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents as their premature disclosure may jeopardize this investigation.

Respectfully submitted,



Shane Robinson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on November 9, 2023



AMANDA MAXFIELD GREEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **(405) 679-8310** (the “**TARGET CELLPHONE**”) whose wireless service provider is **T-MOBILE** (the “**Provider**”), a company that accepts process at **4 SYLVAN WAY, PARSIPPANY, NEW JERSEY 07054**.
2. Records and information associated with the **TARGET CELLPHONE** that is within the possession, custody, or control of the **Provider**.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in **Attachment A** is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the **TARGET CELLPHONE** listed in **Attachment A**:

- a. The following information about the customers or subscribers associated with the **TARGET CELLPHONE** for the time period October 9, 2023, to the present:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long-distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity

Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

- vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address);
- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records;
- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the **TARGET CELLPHONE**, including:
 - 1. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses);
 - 2. information regarding the cell tower and antenna face (also known as “sectors” through which the communication were sent and received; to include the cell tower roundtrip network measurements from tower to device and back to tower, commonly referred to as Timing Advance data (RTT, PCMD, TrueCall, LOCDBOR, etc.).

b. The following information about the customers or subscribers associated with the **TARGET CELLPHONE** for a period of 45 days from the issuance of the warrant, including:

- i. Names (including subscriber names, user names, and screen names);
- ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
- iii. Local and long-distance telephone connection records;
- iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
- v. Length of service (including start date) and types of service utilized;

- vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- c. Prospective information about the location of the cellular phone associated with the **TARGET CELLPHONE** for a period of 45 days (during all times of day and night) from the issuance of the warrant, including:
- i. E-911 Phase II data;
 - ii. GPS data to include cell tower sector information;
 - iii. Latitude-longitude data;
 - iv. Other precise location information, including engineering data to include but not limited to RTT records, PCMD records, Location Database of Records (LOCDBOR) and/or NELOS records, TrueCall records, and all other records containing timing advance measurements and distance-to-tower measurements for all technologies (CDMA, GSM, UMTS, LTE, etc.); and
 - v. Pen Register / Trap and Trace device with prospective cell site information or data about which “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e., faces of the towers) received a radio signal from the **TARGET CELLPHONE** during any voice, SMS, and/or data transmission, including but not limited to engineering data which would include RTT records, PCMD records, Location Database of Records (LOCDBOR) and/or NELOS records, TrueCall records.

II. Information to Be Seized by the Government

All information described above in Section I that would assist and aid in the location of **VARNEY**, as well any evidence of violations of 18 U.S.C. § 2252A, advertise, transport, receive, distribute, possess, and/or access child pornography.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by **T-MOBILE** in order to locate the things particularly described in this Warrant.

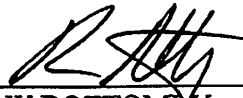
ATTACHMENT C

18 U.S.C. § 3122 Certification

In support of this application, and pursuant to 18 U.S.C. § 3122, I state that I am an “attorney for the Government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure. I certify that the information likely to be obtained from the requested warrant is relevant to an ongoing criminal investigation being conducted by the Investigating Agency of the Target Subject for violation(s) of the Target Offense(s).

I declare under penalty of perjury under the laws of the United States of America that the foregoing paragraph is true and correct.

November 8, 2023
DATE


BOW BOTTOMLY
Assistant United States Attorney